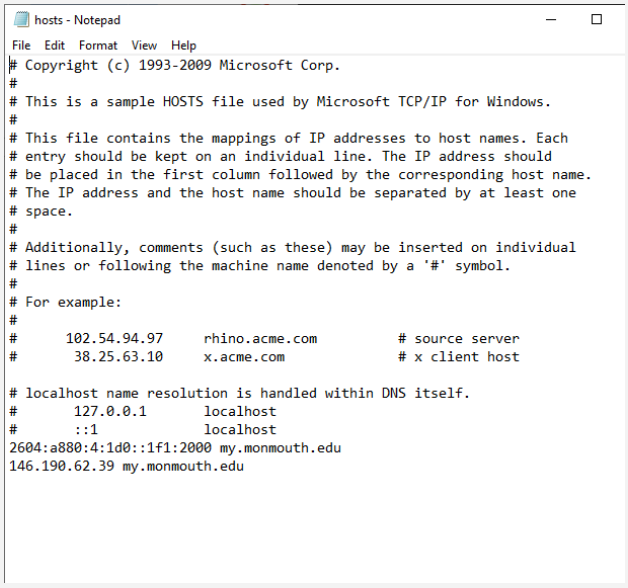
Anjali Narang
CS 450-50
3 December 2024

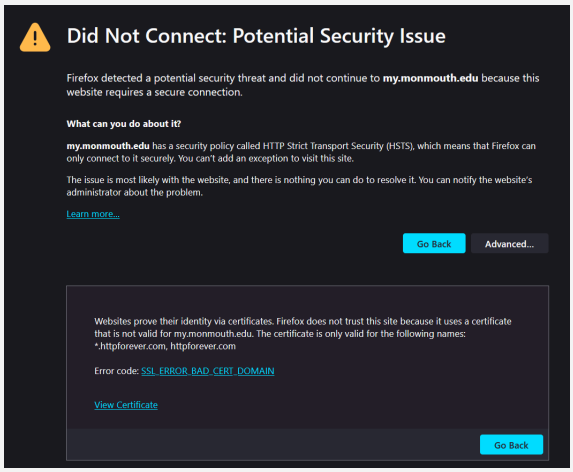
Project Writeup December 3, 2024

I had found that monmouth.edu redirected to httpforever.com perfectly fine in Firefox after configuring the offline-localhost setting in about:config and clearing the DNS and HTTP caches.

However, if the hosts file is as such:

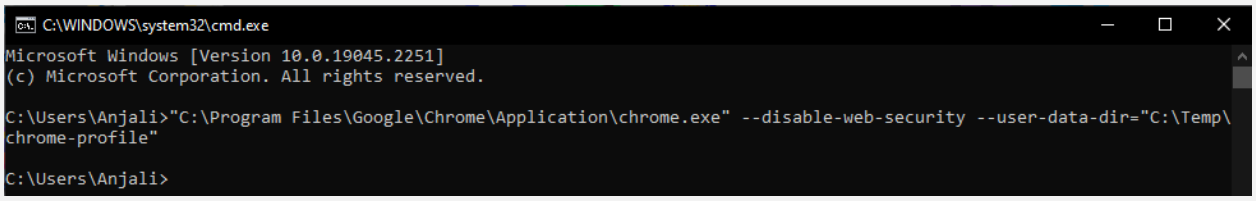


Firefox runs into an issue, since it has strict certificate checking enforced when the website uses HSTS. Unlike other browsers, there is no way for the user to just click “Proceed anyway”.

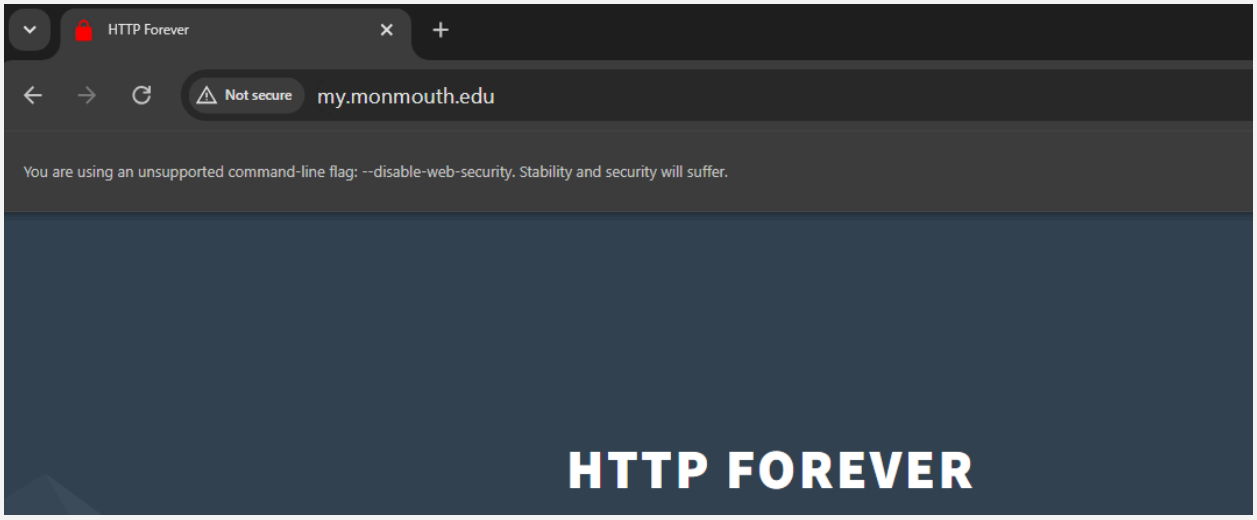


Chrome actually handles the redirect just fine, but it shows httpforever.com in the address bar and not my.monmouth.edu.

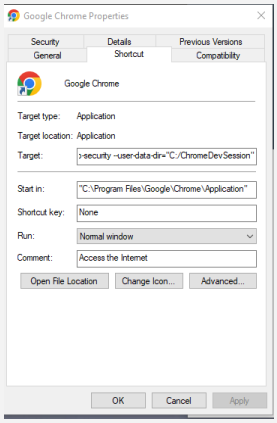
Chrome can be run like this to get it to show my.monmouth.edu in the address bar.



But, it shows a warning to the user on the top of the page:



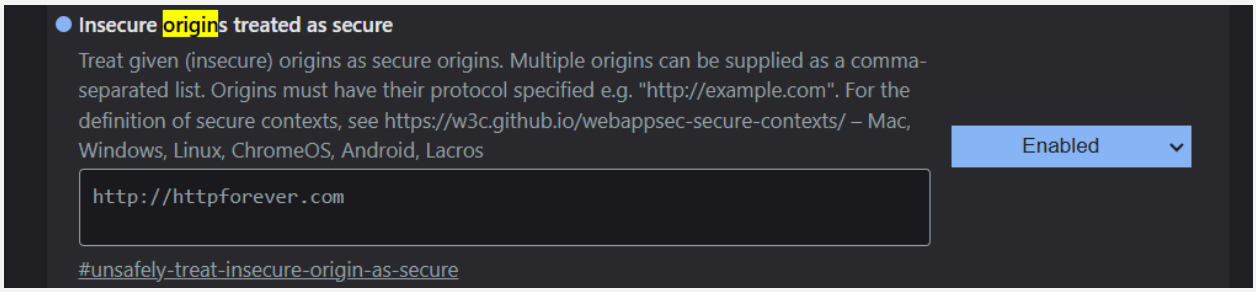
Also, it's not as if the user would run it this way. We would have to somehow get Chrome to run this way whenever the user opens it. I was able to do this by editing the properties of the shortcut, but it shows admin popup every time you open chrome, and the warning still pops up.

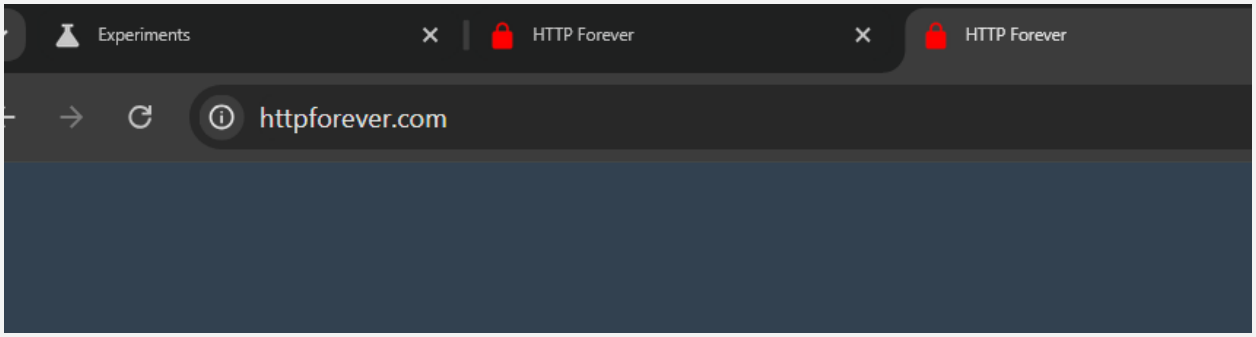


Target: "C:\Program Files\Google\Chrome\Application\chrome.exe" --disable-web-security --user-data-dir="C:/ChromeDevSession"

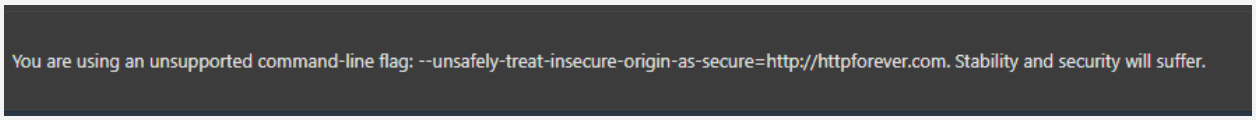
Both this way and the command line way are finicky… It stopped working for me after a bit.

This gets Chrome to show httpforever.com as not insecure:





But this also gave me a warning on the top of the page later.



Interestingly, Chrome only sometimes gives me the warning if I let it be treated as http and try to visit it. When I was first testing this, it gave me the warning the second time I tried to access my.monmouth.edu, then redirected me. Not the first time, and not subsequent times until I reopened the browser.

Pros and Cons

Chrome

Pros:

- do not need to change browser settings to use DNS hosts file (I think)

- cache seemingly does not need to be cleared; reacts to changes in hosts file after restart of browser

Cons:

- does not show my.monmouth.edu in address bar unless we do a lot of fiddling, which also only sometimes works
    - we can ignore this and assume attack victim would not look
- sometimes gives warning trying to access http site

Firefox

Pros:

- redirect is inconspicuous, aside from lock icon in address bar
- does not give warning for trying to access http site

Cons:

- if website to redirect from has HSTS policy, we cannot use it. So, we cannot use my.monmouth.edu (unless we were to setup a server and configure it..)
    - could use monmouth.edu though and redirect it to fake my.monmouth login page? Doesn't make as much sense, but it's an option
    - We can also try to look for something else to use that does not use HSTS
- ducky script needs to handle configuring Firefox settings and clearing cache